We claim:

1. A method for delivering data to a target, the method comprising:

building a data packet, the data packet comprising a header and a payload;

writing data into the payload;

writing processing instructions into the header, and the processing instructions specifying that the data is to be stored in a memory prior to delivery to the target;

providing a computer network, and transmitting the data packet via the computer network;

delivering the data packet via the computer network to a sniffer of a controller, the controller comprising the sniffer and the memory, via the computer network, and coupling the controller to the target;

the sniffer reading the processing instructions, and the sniffer informing the controller to store the data in the memory;

delivering the data via the controller to the memory according to the processing instructions; and

delivering the data from the memory and to the target via the controller.

2. The method of claim 1, wherein the payload comprises target upgrade information.

3. The method of claim 2, wherein the delivery of the upgrade information to the target and the processing instructions specify a time for the delivery of the data to the target.

4. The method of claim 1, wherein said memory is non-volatile memory.

5. The method of claim 4, wherein a first plurality of payloads are stored in a first sector of the memory, and a second plurality of payloads are stored in a second sector of the memory.

6. A method for delivering reprogramming information to a controller, the method comprising:

providing a controller and a target, and coupling the reprogrammable controller and the target,

building a data packet, the data packet comprising a header and a payload;

writing reprogramming data into the payload;

writing processing instructions into the header, and the processing instructions specifying that the data is to be stored in a memory prior to reprogramming the controller;

providing a computer network, and transmitting the data packet via the computer network;

delivering the data packet via the computer network to a sniffer of a controller, the controller comprising the sniffer and the memory, via the computer network;

the sniffer reading the processing instructions, and the sniffer informing the controller to store the data in the memory;

delivering the data via the controller to the memory according to the processing instructions; and

reprogramming the controller by delivering the information stored in the memory to the controller.

7. The method of claim 6, wherein a first sector of the memory holds a first plurality of payloads, and the first plurality of payloads comprises a first set of reprogramming

instructions for the controller, and the controller is reprogrammed by reprogramming the controller with the first set.

8. The method of Claim 7, wherein a second sector of the memory holds a second plurality of payloads, and the second plurality of payloads comprises a second set of reprogramming instructions for the controller, and the controller is reprogrammed by reprogramming the controller with the second set.

9. The method of claim 1, wherein the information contained in the data packet comprises information of one of the types of software or firmware upgrades for the target, remote control monitoring instructions or information, commands, diagnostic software, digital signatures, license identifications, operational histories, status report, status queries, information or measurements relevant to royalty tabulations, firmware enhancements, digital watermarks, monetary or pseudo-monetary tokens or account information, operational limitations or permissions, terms or conditions of licenses, and other suitable types of information, data or instructions known in the art.

10. The method of claim1, wherein the processing instructions direct the controller to transfer the data to the target and bypass the memory.

11. The method of claim 1, further comprising the target peforming a self-test after receiving the data from the controller.

12. The method of claim 11, further comprising a selective delivery of data from the memory after the target fails a self test.

13. The method of claim11, further comprising a notification by the target to the controller of a failure of a self test by the target.

14. The method of claim 1, further comprising;

providing a server and coupling the server to the computer network; and

requiring the target to communicate with server periodically in order for the controller to continue functioning.

15. The method of claim 1, further comprising the provision and use of a hardware accelerator with the controller, whereby the controller speed of operation is increased.

16. The method of claim 1, further comprising the generation of communication transaction identifier records, wherein the message transmitted by the controller over the computer network includes information identifying the message addressee and the message originator.

17. The method of claim 5, further comprising the provision and use of more than two sectors of memory.

18. The method of claim of claim 8, further comprising more than two sets of programming instructions, and storing each set in a separate sector of the memory.

19. The method of claim 1, further comprising the use of a public and private encryption key pair, wherein the data is encrypted with the private key prior to transmission via the computer network and a message controller uses the public key to decrypt the data.

20. The method of claim 1, further comprising the generation and use by the controller of a controller public and private encryption key pair, wherein the controller transmits the controller public key to an addressee, and the controller encrypts a portion of a message with the controller private key, and the controller transmits the message after encryption to the addressee.

21. The method of claim 1, further comprising the authentication of the sender of a message received via the computer network by the controller means of the public key.

22. The method of claim 1, further comprising a reset of the target prior to the delivery of the data to the target.

23. The method of claim 22, further comprising a request for reset signal from the controller to the target and a time out or an acknowledgement signal from the target.

24. The method of claim 22, further comprising a real time clock for use by the controller and target in scheduling the delivery of the data to the target.

25. The method of claim1, the controller further comprising a real time clock.

26. The method of claim 1, further comprising the generation and inclusion of native language commands in the data packet and for use in reprogramming the target.

27. The method of claim 1, further comprising the generation and inclusion of memory mapped data in the data packet and using the memory map data to reprogram the target.

28. A system for reprogramming a target via the Internet, the system comprising:

A server, the server coupled with the Internet;

A controller, the controller comprising a memory;

A target, the target coupled with the controller,

The server for transmitting a plurality of data packets to the controller via the Internet; and

The controller for receiving the plurality of data packets and storing at least a fraction of the data packet in the memory, and the controller reprogramming the target with the fractions of data packets stored in the memory.

29. An apparatus for reprogramming a target, the apparatus comprising:

A sniffer, the sniffer for reading a header of a data packet, and the sniffer storing a payload of the data packet in a memory when directed to by information stored in the header;

The memory for storing the payloads, the memory coupled with the sniffer; and

An upgrade processor for delivering the payloads to the target, the upgrade processor coupled to the memory and the target.

30. The method of claim 1, further comprising the controller retrievably storing the data in the memory in scrambled memory addresses.

31. The method of claim 1, further comprising the controller encrypting the data prior to retrievably storing the data in the memory.

32. The method of claim 1, further comprising the controller encrypting the data prior

to retrievably storing the data in the memory in scrambled memory addresses.

The method of claim 30, further comprising the provision and use of hardware circuitry to enable the retrievable storage of the data in scrambled memory addresses.

33. The method of claim 31, further comprising the provision and use of reconfigurable hardware circuitry to enable the retrievable storage of the data in scrambled memory addresses.

34. The method of claim 30, further comprising the provision and use of reprogrammable software instructions to enable the retrievable storage of the data in scrambled memory addresses.

35. The method of claim 31, further comprising the provision and use of hardware circuitry to enable the encryption of the data prior to retrievable storage of the data in the memory.

36. The method of claim 35, further comprising the provision and use of reconfigurable hardware circuitry to enable the encryption of the data prior to retrievable storage of the data in the memory.

37. The method of claim 31, further comprising the provision and use of reprogrammable software instructions to enable the retrievable storage of the data in the memory.